

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

RoadSync, Inc.,

Plaintiff,

Case No. 1:21-cv-3420-MLB

v.

Relay Payments, Inc., Spencer
Barkoff, James Ryan Droege, and
Does 1–10,

Defendants.

_____/

OPINION & ORDER

Plaintiff RoadSync is a technology company that provides automated solutions to the logistics industry. (Dkt. 1 ¶ 1.) Its signature product is a software platform—called “Checkout”—that streamlines the process of paying companies to load or unload commercial freight. (*Id.* ¶¶ 1, 18–22.) Defendants Barkoff and Droege co-founded Plaintiff and initially served as the company’s Chief Revenue Officer and Chief Operating Officer. (*Id.* ¶¶ 9–10.) But, after a few years, they grew frustrated with the company’s direction, became disruptive, and

threatened to resign. (*Id.* ¶¶ 44–45.) Plaintiff terminated both Defendants as a result. (*Id.* ¶ 50.)

Plaintiff alleges that, one day before their termination, Defendants logged into their work computers and downloaded “the entire RoadSync Google drive” as well as their RoadSync contacts, email, and calendar. (*Id.* ¶¶ 47–48.) Defendants then deleted online records of their download activity, along with several work emails containing Plaintiff’s business information. (*Id.*) Defendants took the downloaded information with them when they left the company. Defendant Droege also took his work-issued laptop, which contained the source code for Checkout. (*Id.* ¶ 51.)

About a year later, Defendants Barkoff and Droege co-founded Defendant Relay as a direct competitor to Plaintiff. (*Id.* ¶ 54.) Defendants hired several of Plaintiff’s employees, targeted Plaintiff’s customers, and eventually launched a payment platform called “Relay” that mimics key features of Plaintiff’s Checkout software. (*Id.* ¶¶ 54–65.) This lawsuit followed.

Plaintiff’s complaint asserts claims for violations of the Federal Defend Trade Secrets Act (“DTSA”) (Count 1), violations of the Georgia Trade Secrets Act (“GTSA”) (Count 2), breach of contract (Counts 3–4),

violations of the Georgia Computer Systems Protection Act (“GCSPA”) (Count 5), and breach of fiduciary duty (Count 6). Defendants move to dismiss these claims in full. (Dkt. 31.) The Court dismisses them only in part.

I. Standard of Review

“To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Id.* This requires more than a “mere possibility of misconduct.” *Id.* at 679. Plaintiff’s well-pled allegations must “nudge[] [his] claims across the line from conceivable to plausible.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007).

II. Doe Defendants

Plaintiff’s complaint names “Does 1–10” as defendants. Defendants say these unidentified parties should be dismissed under the rules governing fictitious party pleading. (Dkt. 31 at 29–30.) The Court agrees.

“As a general matter, fictitious-party pleading is not permitted in federal court.” *Richardson v. Johnson*, 598 F.3d 734, 738 (11th Cir. 2010). There is only one “limited,” “narrow” exception to this rule. *Id.*; *Kabbaj v. John Does 1-10*, 600 F. App’x 638, 641 (11th Cir. 2015). “[P]laintiffs [can] sue real parties under fictitious names only when use of a ‘John Doe’ label is, at the very worst, surplusage because the plaintiff’s description of the defendant is sufficiently clear to allow service of process.” *Vielma v. Gruler*, 808 F. App’x 872, 880 (11th Cir. 2020). So, for example, plaintiffs can sue a Doe defendant described as the “Governor of Alabama” or the “Chief Deputy of the Jefferson County Jail” because those descriptions identify a specific position occupied by only “one person.” *Smith v. Comcast Corp.*, 786 F. App’x 935, 940 (11th Cir. 2019); *Dean v. Barber*, 951 F.2d 1210, 1216 & n.6 (11th Cir. 1992). That is, the descriptions “necessarily pick out one” person for service. *Smith*, 786 F. App’x at 940 (emphasis added). In contrast, descriptions that rely on “vague, widely-shared characteristics,” “general physical attributes,” or “a title that is held by many individuals,” are not enough—even when paired with more detailed allegations about the Doe defendant’s misconduct. *Id.*; *Vielma*, 808 F. App’x at 880. It is insufficient, for

example, to describe a Doe defendant as “a white male [area supervisor at Comcast] with grey hair, a long mustache and a mother of pearl shark’s tooth earring,” who “beat on [plaintiff’s] door loudly, demanded that he step outside, assumed threatening postures, flanked him, and spoke to him in a coarse fashion.” *Smith*, 786 F. App’x at 937, 940; *see also Vielma*, 808 F. App’x at 880.

Plaintiff’s description of Does 1–10 falls squarely into the generic category here. Plaintiff merely refers to them as “officers, employers, agents, or representatives of Relay Payments or the named individual defendants who participated in the theft and misuse of RoadSync’s trade secrets and other confidential information.” (Dkt. 1 ¶ 11; *see id.* ¶¶ 74, 76.) A process server would have no idea who to serve based on this description. That is fatal. *See Vielma*, 808 F. App’x at 880 (dismissing Doe defendants because their “descriptions . . . fall well short of enabling a process server to identify a specific individual”).

Plaintiff insists it could identify Does 1–10 through discovery. (Dkt. 33 at 23.) But the preliminary record does not support that assertion. Plaintiff has already taken three depositions and we still do not know the identities of Does 1–10. (Dkt. 36.) Nor is there any evidence

we are on the verge of finding out. Besides, the Eleventh Circuit “has never permitted John Doe pleading solely on the ground that discovery might reveal an unnamed defendant’s identity.” *Vielma*, 808 F. App’x at 880. “Instead, [Circuit] precedent has always required an unambiguous description of a defendant that enables service of process.” *Id.* Plaintiff’s “sue-first-and-sort-out-the-defendant-later approach is not how litigation works in federal court.” *Id.* at 881. So the Court dismisses Does 1–10.

III. Counts 1–2 (DTSA and GTSA)

Counts 1–2 claim Defendants misappropriated Plaintiff’s trade secrets in violation of DTSA and GTSA. Defendants say these claims should be dismissed for failure to plead a trade secret or misappropriation. The Court partly agrees on the trade-secret issue but disagrees on the misappropriation issue.

A. Trade Secret

To state a claim under DTSA or GTSA, Plaintiff must first identify a plausible trade secret. *U.S. Sec. Assocs., Inc. v. Lumby*, 2019 WL 8277263, at *10 (N.D. Ga. Sept. 25, 2019).¹ Information qualifies as a

¹ The parties agree DTSA and GTSA are “substantially similar and may be addressed together.” (Dkt. 33 at 14; *see* Dkt. 31 at 19, 26–27.) So the

trade secret if “(A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value . . . from not being generally known to, and not being readily ascertainable through proper means by, another person.” 18 U.S.C. § 1839(3); *see* O.C.G.A. § 10-1-761(4).

“[T]rade secrets need not be disclosed in detail” at the pleading stage. *Earthcam, Inc. v. Oxblue Corp.*, 2012 WL 12836518, at *9 (N.D. Ga. Mar. 26, 2012). And “whether something is a trade secret is a question typically resolved by a fact finder after full presentation of evidence from each side.” *Yellowfin Yachts, Inc. v. Barker Boatworks, LLC*, 898 F.3d 1279, 1298 (11th Cir. 2018). But, to survive a motion to dismiss, plaintiff must still “allege sufficient facts to plausibly show a trade secret was involved and to give the defendant notice of the material it claims constituted a trade secret.” *DynCorp Int’l v. AAR Airlift Grp., Inc.*, 664 F. App’x 844, 848 (11th Cir. 2016). This requires “sufficient definiteness to permit a court to apply the criteria for protection.” *TLS*

Court applies the same standards and caselaw to both claims. *See, e.g., Painters Supply & Equip. Co. v. Barkwell*, 2020 WL 7051337, at *2 (N.D. Ga. Dec. 1, 2020) (“The standard required for both claims is substantially identical for the purposes of this Order.”).

Mgmt. & Mktg. Servs., LLC v. Rodriguez-Toledo, 966 F.3d 46, 53 (1st Cir. 2020).

Plaintiff claims Defendants misappropriated four categories of trade secrets. The Court considers each.

1. Customer Information

The first category is customer lists, customer data compilations, and prospective customer lists. (Dkt. 1 ¶¶ 25, 49.) Defendants say this information is not a trade secret because Plaintiff “fails to plead . . . its customers are not publicly known or ascertainable.” (Dkt. 31 at 23.) The Court disagrees. The complaint alleges (1) Plaintiff’s customers are part of “a fragmented industry that includes many obscure small- and mid-sized players”; (2) Plaintiff “invested years of effort and thousands of employee hours, and made a significant monetary investment, to create competitive market intelligence to identify players in the relevant fragmented markets . . . and establish relationships with customers and prospective customers”; and (3) “[t]he substantial investment[] required to enter and grow in th[e] industry has resulted in relatively few competitors.” (Dkt. 1 ¶¶ 23, 27.) This reasonably suggests Plaintiff’s

customers are not “generally known” or “readily ascertainable” as required by DTSA and GTSA.

Defendants also claim “knowledge on the part of [an] employee concerning the names and addresses of customers” is not a trade secret. (Dkt. 31 at 24.) But this argument fails as well. Defendants took more than just “names and addresses.” They took information about key contacts, decision-makers, volumes, proposed and acceptable prices, payment and purchase histories, contact history, and potential revenue. (Dkt. 1 ¶¶ 25, 49.) At least that is what Plaintiff alleges. This is exactly the kind of “specific, highly-detailed [customer] information” Defendants’ own cases say is enough. (Dkt. 31 at 24.) Moreover, Plaintiff’s theory is that Defendants physically downloaded this information from tangible sources. So Defendants’ distinction between “intangible knowledge” (which cannot be a trade secret) and “a tangible document” (which can) simply does not apply here. (Dkt. 31 at 25.) Plaintiff has plausibly alleged its customer information is a trade secret. *See Corp. Ins. Advisors, LLC v. Addeo*, 2022 WL 2718140, at *5 (S.D. Fla. June 27, 2022) (“Databases and lists with client information are typically seen as protectable trade secrets.”); *see, e.g., Howmedica Osteonics Corp. v.*

Alphatec Spine, Inc., 2022 WL 3136837, at *7 (M.D. Fla. June 17, 2022) (plaintiff adequately alleged a trade secret by referring to “customer lists, customer purchasing patterns, customer preferences, [and] customer operating room protocol”).

2. Source Code

Plaintiff’s second trade-secret category is “source code for RoadSync’s Checkout (including its Remote Checkout and robodialer functionality) and related software (including the ‘paycodes’ functionality used for Remote Checkout).” (Dkt. 1 ¶ 25.) Defendants say this description is either too vague or “so broad[] as to indisputably sweep in vast amounts of public material.” (Dkt. 38 at 10 n.4.) The Court disagrees.

Starting with the too-vague argument, plaintiffs need only allege “the general nature of [any] Software” or related computer information for which they seek trade-secret protection. *Protegrity Corp. v. Elavon Inc.*, 2018 WL 8949789, at *2 (N.D. Ga. Aug. 22, 2018). Plaintiff has done that here. It seeks to protect “source code” for three Checkout functionalities (Remote Checkout, robodialer, and paycodes) that are fairly described in the complaint. (See Dkt. 1 ¶¶ 18–22, 58–60 (discussing

Checkout and the functionalities).) Courts routinely find such allegations sufficient. *See, e.g., Advanced Concept Innovations, LLC v. Kimberly-Clark Glob. Sales, LLC*, 2021 WL 8084310, at *3 (M.D. Fla. Oct. 29, 2021) (finding sufficient a reference to “software . . . used to manufacture and package the general purpose face masks and general purpose N95 specified by the Defendants”); *Sentry Data Sys., Inc. v. CVS Health*, 361 F. Supp. 3d 1279, 1294 (S.D. Fla. 2018) (finding sufficient a reference to “proprietary software programs for administering the 340B program”).²

Defendants’ public-information argument also fails. Defendants say Checkout’s “outward-facing features do not qualify as trade secrets because they can be viewed by anyone using the product.” (Dkt. 31 at 26.) But Plaintiff does not claim its “outward-facing features” are trade secrets. (Dkt. 33 at 21.) It claims the source code *underlying* those

² *See also Protegrity*, 2018 WL 8949789, at *1–2 (“tokenization software . . . and the documentation accompanying the software” adequately identified a trade secret); *Autodesk, Inc. v. ZWCAD Software Co.*, 2015 WL 2265479, at *5 (N.D. Cal. May 13, 2015) (finding sufficient a reference to “the source code which comprises AutoCAD 2007 and 2008 . . . , including those portions of code that underlie the commands, interfaces and program files associated with the dozens of specific features which were wrongfully acquired and used in Defendants’ ZWCAD+ 2012 and 2014 programs”).

features is protected. The “distinction between source code and the visible output of [a] software program” is well established. *AirWatch LLC v. Mobile Iron, Inc.*, 2013 WL 4757491, at *4 (N.D. Ga. Sept. 4, 2013) (Carnes, J.). The latter includes “[t]hings that any user or passer-by [can] see[],” which precludes trade-secret protection. *Fin. Info. Techs., LLC v. iControl Sys., USA, LLC*, 21 F.4th 1267, 1273 (11th Cir. 2021). But the former is “*not* accessible” to a program user, “is not readily ascertainable,” and is “generally considered to be a trade secret.” *Warehouse Sols., Inc. v. Integrated Logistics, LLC*, 2014 WL 12647878, at *6 (N.D. Ga. July 7, 2014); *see Fin. Info.*, 21 F.4th at 1273 (“As a general matter, software source code is not readily ascertainable and, accordingly, qualifies for trade-secret protection.”).³

Defendants never identify any information in Plaintiff’s source code—as opposed to Plaintiff’s outward-facing software—that is even arguably public. And, even if they had, that would not be dispositive.

³ “A software program’s source code is written in a programming language, after which a compiler converts the source code into object code. A computer will then execute the object code in a manner that makes the program cognizable for human users, resulting in the end-product (i.e., what the user perceives as the software, the program, or the ‘system’).” *Warehouse*, 2014 WL 12647878, at *6.

A “unique combination” of public information counts as a trade secret if it “adds value to the information.” *See Penalty Kick Mgmt. Ltd. v. Coca Cola Co.*, 318 F.3d 1284, 1291 (11th Cir. 2003) (“The fact that some or all of the components of the trade secret are well-known does not preclude protection for a secret combination, compilation, or integration of the individual elements.”). No one claims the underlying source code for Checkout is not unique or valuable as an overall package. And the complaint plausibly suggests it is. *See Verbena Prod. LLC v. Del Toro*, 2022 WL 910666, at *3 (S.D. Fla. Mar. 29, 2022) (“[S]oftware configurations can constitute trade secrets.”). Certainly on the record here, the extent to which Plaintiff’s source code is in the public domain—and the significance of any such publicness—are questions of fact best left for summary judgment or trial. *See Mile High Healthcare Analytics, LLC v. Med. Care Consortium Inc.*, 2020 WL 9460325, at *10 (S.D. Fla. July 29, 2020) (“The law is clear that questions of fact cannot be resolved on motions to dismiss.”). Plaintiff adequately alleges its source code is a trade secret.⁴

⁴ Notably, Defendants do not dispute Plaintiff’s source code includes at least *some* confidential information that qualifies as a trade secret. *See*

3. Product Information and Financial Analyses

The final two categories of alleged trade secrets are (1) “product road maps, workflows, and confidential user guides,” and (2) “financial analyses (including pricing, costs, economic models, and forecasts).” (Dkt. 1 ¶¶ 25, 49.) Defendants say these descriptions are too vague to plead a plausible trade secret. (Dkt. 31 at 20–23.) The Court agrees.

Not all “financial and technical data” is secret or derives economic value from its secrecy. *DynCorp*, 664 F. App’x at 849; see *Brightview Grp., LP v. Teeters*, 2021 WL 1238501, at *5 (D. Md. Mar. 29, 2021) (“[N]ot all financial information or business planning and operational materials qualify as trade secrets.”). The same goes for “[a]ll information concerning a product.” *VVIG, Inc. v. Alvarez*, 2019 WL 5063441, at *4 (S.D. Fla. Oct. 9, 2019). Thus, courts have dismissed claims seeking trade-secret protection for “product specifications,” “roadmaps,” “financial affairs,” “accounting statistical data,” “pricing data,” “particularized costing information,” “sales data,” “sales projections,” and

Deloitte Tax LLP v. Murray, 2022 WL 1406612, at *5 (N.D. Ohio May 4, 2022) (“Confidential source code clearly meets the definition of a trade secret.”) (collecting authorities).

“product forecasts.”⁵ These “broad categories of information” were insufficient because they did not “show a trade secret was involved” or “give the defendant notice of the material [plaintiff] claim[ed] constituted a trade secret.” *DynCorp*, 664 F. App’x at 848.

So too here. The Court has no idea what Plaintiff means by “road maps” and “workflows.” And the complaint refers only to the broadest components of financial analyses, using vacuous labels that could refer to pretty much anything. “User guide” is a more meaningful label. But Plaintiff never explains why the information in its *user* guides is not “readily ascertainable” by its product *users*. See *Medicrea USA, Inc. v. K2M Spine, Inc.*, 2018 WL 3407702, at *13 (S.D.N.Y. Feb. 7, 2018) (“[S]ale of a product . . . may place that product or information about how it works in the public domain.”). Without more, the Court simply cannot determine whether Plaintiff’s “broad categories of [financial and product]

⁵ See *Agile Sourcing Partners, Inc. v. Dempsey*, 2021 WL 4860693, at *7 (C.D. Cal. July 15, 2021) (“pricing data”); *Vital Pharms., Inc. v. Alfieri*, 2021 WL 9098064, at *3 (S.D. Fla. July 2, 2021) (“sales data”); *Profade Apparel, LLC v. Rd. Runner Sports, Inc.*, 2020 WL 5230490, at *4 (S.D. Cal. Sept. 2, 2020) (“roadmap”); *Power Integrations, Inc. v. Silanna Semiconductor N. Am., Inc.*, 2020 WL 3508078, at *3 (D. Del. June 29, 2020) (“product specifications,” “product forecasts,” “particularized costing information,” and “marketing and sales projections”); *VVIG*, 2019 WL 5063441, at *4 (“financial affairs” and “accounting statistical data”).

information” plausibly meet the definition of a trade secret. *DynCorp*, 664 F. App’x at 849. That is fatal under DTSA and GTSA. *See DeCurtis LLC v. Carnival Corp.*, 2021 WL 1540518, at *3 (S.D. Fla. Apr. 20, 2021) (“[T]here is no error in requiring a plaintiff to provide some specifics in order to state a claim for the misappropriation of trade secrets.”).

B. Misappropriation

Plaintiff has adequately identified several trade secrets. But, to state a claim, Plaintiff must also show Defendants “misappropriated” those trade secrets. *Lumby*, 2019 WL 8277263, at *10. DTSA and GTSA define misappropriation as “(A) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or (B) disclosure or use of a trade secret of another without express or implied consent” 18 U.S.C. § 1839(5); O.C.G.A. § 10-1-761(2). This means “[t]here are three ways to establish misappropriation . . . : improper acquisition, disclosure, or use of a trade secret without consent.” *Oakwood Lab'ys LLC v. Thanoo*, 999 F.3d 892, 907–08 (3d Cir. 2021).

Defendants Barkoff and Droege say their alleged downloading of the trade secrets just before leaving the company does not constitute

improper acquisition because they had the right to access it while employed. (Dkt. 31 at 27.) And, they say the complaint fails to plead they “used” Plaintiff’s trade secrets without consent. (*Id.* at 28–29.) The Court disagrees with this second assertion and concludes there is enough in the complaint to support a plausible inference of misuse. *See Perma-Liner Indus., LLC v. D’Hulster*, 2022 WL 772736, at *3 (M.D. Fla. Feb. 9, 2022) (“[T]he bar for what counts as ‘use’ of a trade secret is generally low.”).⁶ Defendants downloaded virtually all the trade secrets one day before they left the company, within eight minutes of one another, when they “understood [they] were at imminent risk of termination.” (Dkt. 1

⁶ Because Plaintiff adequately pleads misappropriation under an improper-use theory, the Court need not decide whether Plaintiff also pleads misappropriation under an improper-acquisition theory. Certainly Defendant Droege “acquired” Plaintiff’s source code “by improper means” when he stole the company laptop on which that code was stored. *See* 18 U.S.C. § 1839(5)–(6); O.C.G.A. § 10-1-761(1)–(2) (both defining “improper means” to include “theft”). But it is less clear whether Defendants acquired Plaintiff’s other trade secrets by improper means when they downloaded that information during their employment with Plaintiff. *See Angel Oak Mortg. Sols. LLC v. Mastronardi*, 2022 WL 875910, at *7 & n.9 (N.D. Ga. Mar. 23, 2022) (discussing the difficulties of proceeding under this theory on similar facts). So the Court takes no view today as to whether Defendants’ furtive efforts to acquire Plaintiff’s information while walking out the door cannot constitute improper acquisition as a matter of law simply because they were generally authorized to access that information while employed.

¶¶ 45–49.) They tried to hide what they did by deleting Plaintiff’s records. (*Id.* ¶¶ 47–48.) Defendant Droege stole a company laptop containing the source code for Checkout. (*Id.* ¶ 51.) He refused to give it back when asked. (*Id.* ¶¶ 52–53.) Neither Defendant returned Plaintiff’s other trade secrets when asked. (*Id.*) Instead, they started a competing company only one year later. (*Id.* ¶ 54.) All of this demonstrates, at least, Defendants’ intent to do something with the trade secrets without Plaintiff’s consent.

Defendants then hired several of Plaintiff’s employees, including key engineers who worked on Checkout. (*Id.* ¶ 54, 62, 99.) They partnered with one of Plaintiff’s customers to develop a product that Plaintiff and the customer had been collaborating on earlier that year. (*Id.* ¶ 54.) And, within just a couple of years, they launched a payment platform called “Relay” that mimics key features of Plaintiff’s Checkout software. (*Id.* ¶ 54.) Defendants do not disclose these features on their company website. (*Id.* ¶¶ 4, 56.) They offer some of them for free or at deeply discounted prices. (*Id.* ¶ 57.) And they actively target Plaintiff’s customers. (*Id.* ¶¶ 4, 54, 63.)

Given the totality of these allegations, and viewing them in Plaintiff's favor, the complaint adequately pleads that Defendants "used" Plaintiff's trade secrets to compete with Plaintiff and that they did so "without express or implied consent." That meets the legal test for misappropriation under both DTSA and GTSA. *See, e.g., Integral Dev. Corp. v. Tolat*, 675 F. App'x 700, 703 (9th Cir. 2017) (a jury could find Tolat misappropriated Integral's source code because "Tolat copied the source code shortly before he planned to leave Integral and join EBS" and "EBS [later] released a product . . . that competed directly with some of Integral's products"); *Verbena*, 2022 WL 910666, at *4 ("Given that [plaintiff] . . . started his own competitive ecommerce business—selling the same products [his former employer] sold—mere months after [the former employer] investigated him for stealing inventory, it is plausible to infer that [plaintiff] improperly used the trade secrets."); *see also AirWatch*, 2013 WL 4757491, at *5 ("While plaintiff does not allege how exactly defendant is using the information it acquired, [plaintiff's] allegation that [defendant] acquired the program and is using it to develop its own products is sufficient at the motion to dismiss stage.").

C. Conclusion

The Court dismisses Counts 1–2 to the extent they claim Defendants misappropriated Plaintiff’s “financial analyses (including pricing, costs, economic models, and forecasts)[,] product road maps, workflows, and confidential user guides.” (Dkt. 1 ¶ 25, 49.) Counts 1–2 can otherwise proceed.

IV. Count 3 (Breach of Contract)

Count 3 claims Defendants Barkoff and Droege violated several confidentiality and non-solicitation provisions in their 2016 employment agreement with Plaintiff. Defendants say this claim should be dismissed because the relevant provisions in the agreement are unenforceable under California law. The Court disagrees.

To resolve Defendants’ argument, the Court must first determine whether California law applies here. Everyone agrees Georgia’s choice-of-law rules control that inquiry. *See Stohs v. NewRez, LLC*, 2020 WL 3317710, at *5 (N.D. Ala. June 18, 2020). Those rules say “contract [claims] are governed by the substantive law of the state where the contract was made.” *Rayle Tech, Inc. v. DEKALB Swine Breeders, Inc.*, 133 F.3d 1405, 1409 (11th Cir. 1998). But they also say “parties by

contract may stipulate that the laws of another jurisdiction will govern the transaction.” *Id.* That is what the parties did here. They included a California choice-of-law provision in their agreement.⁷ “Georgia law ordinarily honors [such] provisions.” *Metro. Life Ins. Co. v. Tucker*, 846 F. App’x 798, 800 (11th Cir. 2021). But not always.

Plaintiff claims this is one of those cases where Georgia would not honor the parties’ choice-of-law provision. It says that is so because the parties’ chosen jurisdiction—California—has “no substantial relationship to the parties or events.” (Dkt. 33 at 30–31.) Defendants’ only response to this argument appears in a two-sentence footnote. That is not enough to contest the point. *See Pinson v. JPMorgan Chase Bank, Nat’l Ass’n*, 942 F.3d 1200, 1209 n.5 (11th Cir. 2019) (“We do not ordinarily consider arguments raised in passing in one footnote rather than the body of the brief.”); *Taser Int’l, Inc. v. Phazzer Elecs., Inc.*, 2020

⁷ The provision reads: “The validity, interpretation, construction and performance of this Agreement, and all acts and transactions pursuant hereto and the rights and obligations of the parties hereto shall be governed, construed and interpreted in accordance with the laws of the state of California, without giving effect to the principles of conflict of laws.” (Dkts. 1-1 at 9; 1-2 at 9.)

WL 13104165, at *4 n.2 (M.D. Fla. Aug. 10, 2020) (“The Court generally does not consider arguments raised in a footnote.”).

Defendants’ footnote also fails on the merits. It claims the Georgia Supreme Court does not require “the selected state’s laws [to] have a substantial relationship to the parties or transaction.” (Dkt. 38 at 17 n.11.) But the Georgia Supreme Court has never explicitly said that. And, for over 30 years, the Eleventh Circuit has repeatedly said the opposite.⁸ So have countless other district court judges in this state.⁹

⁸ See, e.g., *Bearden v. E.I. du Pont de Nemours & Co.*, 945 F.3d 1333, 1338 (11th Cir. 2019) (“Georgia law ordinarily honors choice-of-law provisions, and Bearden offers no evidence that [the chosen jurisdiction] bears no substantial relationship to the parties or the transaction. So we will respect the parties’ choice of law.”); *Rayle*, 133 F.3d at 1409 (“[P]arties by contract may stipulate that the laws of another jurisdiction will govern the transaction, unless . . . the chosen jurisdiction has no substantial relationship to the parties or the transaction.”); *Velten v. Regis B. Lippert, Intercat, Inc.*, 985 F.2d 1515, 1519 (11th Cir. 1993) (“Parties are permitted to stipulate that another jurisdiction’s law will apply, unless . . . the jurisdiction has no substantial relationship to the parties or the transaction.”); *Johnson v. Occidental Fire & Cas. Co. of N. Carolina*, 954 F.2d 1581, 1584 (11th Cir. 1992) (noting “Georgia’s conflict of law rules” consider whether “a state has no substantial relationship to the parties or the transaction”).

⁹ See, e.g., *Patel v. Ragland*, 2019 WL 13211814, at *5 (N.D. Ga. Nov. 1, 2019) (Totenberg, J.) (“Parties . . . may stipulate that the laws of another jurisdiction will govern the transaction, unless the . . . chosen jurisdiction has no substantial relationship to the parties or the transaction.”); *Access Point Fin., Inc. v. Ext-Indy Suites, LLC*, 2018 WL 2971182, at *2 (N.D.

Indeed, just last year, the Eleventh Circuit confirmed “[a] choice-of-law provision will not be upheld [in Georgia] if . . . the chosen jurisdiction has no substantial relationship to the parties or the transaction.” *Tucker*, 846 F. App’x at 800. That has been the mantra in this Circuit since at least 1992. And, given the terseness of Defendants’ argument, the Court is not inclined to cut a new path today.¹⁰

That being so, the outcome here is clear. Nothing in the complaint suggests California has a “substantial relationship”—or even *any* relationship—to the parties or events in this case. Defendants do not

Ga. June 13, 2018) (Story, J.) (“[I]f the chosen state has no substantial relationship to the parties or the transaction, the chosen law will not be applied.”); *Deutz Corp. v. Engine Distributors, Inc.*, 2017 WL 11692626, at *3 (N.D. Ga. May 12, 2017) (Batten, J.) (“[A] court will not apply the parties’ chosen law if the chosen state has no substantial relationship to the parties or the transaction.”); *Cold Chain Techs., Inc. v. IGH Holdings, Inc.*, 2015 WL 12778346, at *2 (N.D. Ga. Aug. 5, 2015) (Jones, J.) (“[S]tipulations are enforced, unless the . . . chosen jurisdiction has no substantial relationship to the parties or the transaction.”); *Gen. Motors LLC v. Canton Motor Sales, Inc.*, 2014 WL 901430, at *7 (N.D. Ga. Mar. 7, 2014) (Carnes, J.) (“Georgia law will not follow the law of the state stipulated to by the parties . . . if that state has no substantial relationship to the parties or the transaction at issue.”); *see also S. Felt Co., Inc. v. Konesky*, 2020 WL 5199269, at *4–5 (S.D. Ga. Aug. 31, 2020) (Hall, C.J.) (discussing and applying the “substantial relationship” test).

¹⁰ The Court is open to revisiting this issue on a better record. The Court’s own research has revealed several reasons to question the Eleventh Circuit’s position. But, at this early stage of the case, with such little input from the parties, now is not the right time to get into it.

dispute that. So the California choice-of-law provision is unenforceable. That means California law does not apply. And, since Defendants' motion to dismiss Count 3 is based entirely on California law, Count 3 can proceed.

V. Count 4 (Breach of Contract)

Count 4 claims Defendant Droege violated confidentiality provisions in his 2018 employment agreement with Plaintiff. Defendant says this claim should be dismissed because he owes “the same” confidentiality obligations to Plaintiff under his 2016 agreement, meaning the provisions in his 2018 agreement lack a “legitimate business purpose.” (Dkt. 31 at 41–43.) The Court disagrees.

Under Georgia law—which everyone agrees applies here—“[t]he person seeking enforcement of a restrictive covenant shall plead and prove the existence of one or more legitimate business interests justifying the restrictive covenant.” O.C.G.A. § 13-8-55. “Legitimate business interests include, but are not limited to, protecting trade secrets and valuable confidential information that otherwise does not qualify as a trade secret.” *IVC US, Inc. v. Huali Grp. (U.S.), LLC*, 2021 WL 2561774, at *3 (N.D. Ga. Apr. 2, 2021). The 2018 agreement clearly offers this

protection because it prohibits Defendant from disclosing or misusing “Confidential Information” and requires him to return “Confidential Information” upon his termination or at Plaintiff’s request. (Dkt. 1 ¶ 42.) No one disputes that. Defendant simply notes the 2016 agreement offers “duplicative” protection. (Dkt. 31 at 41.) Defendant claims that is not allowed under Georgia law.

Defendant’s only support for this theory—that double-protection destroys a “legitimate business interest” that would otherwise exist—is *Am. Software USA, Inc. v. Moore*, 448 S.E.2d 206 (Ga. 1994). But the narrow issue in *Moore* was whether a nationwide noncompete clause was “unreasonably expansive.” *Id.* at 208. It is entirely unclear whether the Georgia Supreme Court’s answer to that limited question can support the broader proposition advanced by Defendant here.

Even if it could, Defendant’s argument would still fail because the 2018 agreement does not “merely duplicate[]” the 2016 agreement as Defendant contends. (Dkt. 31 at 12.) It offers broader protection. (*See* Dkt. 1 ¶¶ 37–42.) For example, the 2018 agreement arguably requires Defendant to return a wider array of confidential materials than the 2016 agreement (“Confidential Information” vs. “documents or property”). It

requires Defendant to return those materials in a broader set of circumstances (“upon the earlier of a request by the Company or termination” vs. “at the time of termination”). And it includes a cooperation clause that does not appear in the 2016 agreement (“I will cooperate with the Company and use my best efforts to prevent the unauthorized disclosure of all Confidential Information”). Plaintiff pointed this out in its response brief. (Dkt. 33 at 35 & n.10.) Defendant never addressed the issue in his reply. (Dkt. 38 at 20.)

To be sure, the two agreements do overlap. But Defendants never claim—not clearly, anyway—that *some* overlap is a problem. And, even if they had, that argument would be a hard sell. Contract drafters routinely “adopt a belt-and-suspenders approach to try to capture the universe,” including in the restrictive-covenant context. *Reid Hosp. & Health Care Servs., Inc. v. Conifer Revenue Cycle Sols., LLC*, 8 F.4th 642, 652 (7th Cir. 2021); see *Infinity Cap. LLC v. Francis David Corp.*, 851 F. App’x 579, 588–89 (6th Cir. 2021) (discussing this approach in connection with non-solicitation provisions). And, for the most part, “nothing prevents” them from doing so. *Infinity*, 851 F. App’x at 588–89. A rule

that requires *no* overlap—upon penalty of unenforceability—would be strong medicine. And probably unrealistic.

Given the preliminary posture of this case, the uncertain scope of Defendant’s cited authority, the fact that the 2018 agreement protects confidential information as required by Section 13-8-55, the fact that it does so more extensively than the 2016 agreement (at least in some respects), and Defendant’s failure to meaningfully explore these issues in its briefing, the Court declines—at this stage—to say the 2018 agreement has no legitimate business interest. Count 4 can proceed.

VI. Count 5 (GCSPA)

Count 5 claims Defendants Barkoff and Droege improperly used Plaintiff’s computer network and computers in violation of the GCSPA. Defendants say this claim should be dismissed because it is preempted by GTSA and fails to state a claim. The Court concludes GTSA preempts part of Count 5, but that the surviving portion adequately states a claim.

A. Preemption

“GTSA preempts claims that rely on the same allegations as those underlying the plaintiff’s claim for misappropriation of a trade secret.” *Robbins v. Supermarket Equip. Sales, LLC*, 722 S.E.2d 55, 58 (Ga. 2012);

see O.C.G.A. § 10-1-767(a). Plaintiff's GCSPA claim runs afoul of this rule. It alleges Defendants impermissibly used Plaintiff's computer network and computers to misappropriate Plaintiff's trade secrets. (Dkt. 1 ¶¶ 115–116.) Plaintiff's GTSA claim relies on the same allegation. (*Id.* ¶¶ 70, 82, 85.) So, to that extent, GTSA preempts Count 5. See *Argos USA LLC v. Young*, 2019 WL 4125968, at *12 (N.D. Ga. June 28, 2019) (finding GTSA preemption because “Plaintiff relies on the same factual allegations of misappropriation for its GCSPA [claim] as its GTSA claim. Specifically, Plaintiff relies on facts that Young used Plaintiff's computer system to misappropriate Plaintiff's proprietary information.”); *Agilysys, Inc. v. Hall*, 258 F. Supp. 3d 1331, 1349 (N.D. Ga. 2017) (GTSA preempted GCSPA claim because “Plaintiff relies on the same factual allegations of misappropriation for [both claims], namely, that [Defendant] used Plaintiff's computer system without authorization or in excess of his authorization to misappropriate Plaintiff's proprietary information”).

But Count 5 also alleges Defendants impermissibly used Plaintiff's computer network and computers to *delete* work emails containing company information. (Dkt. 1 ¶¶ 118–119.) Plaintiff's GTSA claim does

not rely on this allegation. (*See id.* ¶¶ 66–90.) So, to that extent, Count 5 survives GTSA preemption. *See NCR Corp. v. Pendum, LLC*, 2018 WL 11343391, at *12 (N.D. Ga. Aug. 8, 2018) (GTSA preempted tortious interference claim “to the extent” the claim “relies on allegations of the use of NCR’s trade secrets” but not to the extent it alleges interference “in other ways”). Count 5 also survives to the extent it is based on Defendants’ theft of Plaintiff’s laptop rather than Defendants’ theft of the information stored on that laptop. This is a tricky distinction but courts in Georgia—and around the country—continue to make it. No one asks the Court to do otherwise here. *See Tronitec, Inc. v. Shealy*, 547 S.E.2d 749, 755 (Ga. Ct. App. 2001) (GTSA preempted claims for conversion and theft “to the extent [they] were limited to trade secrets” but not to the extent they involved “a personal computer [that was] not a trade secret”); *Infinite Energy, Inc. v. Catalyst Energy, LLC*, 2007 WL 9702596, at *5 (N.D. Ga. Aug. 16, 2007) (“If Infinite was seeking return of tangible property of value apart from the information contained therein, such as

a computer containing confidential information, its conversion claim could feasibly avoid preemption.”).¹¹

Plaintiff argues GTSA does not preempt Count 5 to the extent it alleges “theft of confidential, *non-trade secret* data.” (Dkt. 33 at 24 (emphasis added).) But what data is Plaintiff talking about? The only stolen data identified in the complaint is the alleged trade-secret information for which Plaintiff seeks protection under GTSA. (Dkt. 38 at 14; see Dkt. 1 ¶¶ 25, 49.) Having sought relief under GTSA for that information, Plaintiff cannot now “plead a lesser and alternate theory of

¹¹ See also *Snapkeys, Ltd. v. Google LLC*, 442 F. Supp. 3d 1196, 1208 (N.D. Cal. 2020) (“Snapkeys’ conversion claim survives only insofar as Snapkeys seeks recovery for the value of its tangible physical property, rather than the value of the trade secrets or any other confidential information embedded in those prototypes.”); *Mauser USA, LLC v. Wilburn*, 2019 WL 8376209, at *7 (N.D. Ga. Nov. 22, 2019) (“Had Mauser in fact alleged that Wilburn refused to return his work-issued laptop and cell phone, a conversion claim based on these allegations would not be preempted under the GTSA as the laptop and cell phone would have value apart from the proprietary information contained within them and could be repurposed for use by another Mauser employee.”); *Source Prod. & Equip. Co. v. Schehr*, 2017 WL 3721543, at *7 (E.D. La. Aug. 29, 2017) (“[T]o the extent plaintiffs seek to recover the physical value of their thumb drives and CDs from Schehr, their conversion claim is not preempted. To the extent plaintiffs seek to recover the value of the trade secrets contained within this physical property, their conversion claim is preempted.”).

restitution simply because the information does not qualify as a trade secret.” *Robbins*, 722 S.E.2d at 58.

Count 5 is preempted to the extent it is based on Defendants’ misappropriation of data but not to the extent it is based on Defendants’ deletion of data or conversion of Plaintiff’s physical laptop.

B. Merits

To prevail on its non-preempted GCSPA claims, Plaintiff must show Defendants “use[d] a computer or computer network with knowledge that such use [was] without authority.” O.C.G.A. § 16-9-93(a)–(b). Defendants do not dispute Plaintiff has made this showing with respect to its stolen-physical-laptop theory. But they say the “without authority” element is missing from Plaintiff’s email-deletion theory. Their argument is simple: employees have “general authority” to delete their work emails. (Dkts. 31 at 31–33; 38 at 14–15.) That is true, of course. But it is hardly dispositive. The fact that employees *generally* have authority to do something does not mean they *always* do.

DuCom v. State, 654 S.E.2d 670 (Ga. Ct. App. 2007) makes that clear. There, an employee logged into her work computer and downloaded confidential client information. She had the authority to do

that “as a part of her [job] duties.” *Id.* at 676. But she did not have the authority to do it for “personal use” or to benefit a competitor. *Id.* at 672, 676. The evidence suggested she did it for those improper purposes. *Id.* at 676. So the court held a jury could conclude she used the computer “without authority” in violation of the GCSPA. *Id.*

The same is true here. Defendants may have had “general authority” to delete their work emails in the ordinary course of their employment. (Dkt. 31 at 33.) But they did not have authority to do so for the improper purpose of benefitting themselves and harming the company. Both Defendants signed contracts to that effect. (*See, e.g.*, Dkt. 1 ¶ 35 (“I will devote my best business efforts to the interests of the Company and will not engage in other employment or in any activities detrimental to the best interests of the Company without the prior written consent of the Company.”).) So, when Defendants deleted their emails “to cover up their theft” and “leav[e] RoadSync competitively disadvantaged,” they used their work computers in violation of their contractual obligations. (Dkt. 1 ¶¶ 120, 125.) And that means they “use[d] a computer . . . without authority” under GCSPA. O.C.G.A. § 16-9-93(b); *see G.W. Henssler & Assocs., Ltd. v. Marietta Wealth Mgmt., LLC*,

2017 WL 6996372, at *5 (N.D. Ga. Oct. 23, 2017) (noting an employee who uses a computer in violation of his “contractual obligations” acts “without authority” under GCSPA); *IPC Sys., Inc. v. Garrigan*, 2012 WL 12872028, at *10 (N.D. Ga. May 21, 2012) (“Defendant was not authorized to access confidential business information on [his employer’s] computers for nonbusiness related reasons and therefore, if [he did that], he exceeded his authorized access to [the] computers for an alleged improper purpose in violation of the GCSPA.”).¹²

C. Conclusion

Count 5 can proceed to the extent it asserts a GCSPA claim based on Defendants’ deletion of data and Defendants’ theft or conversion of Plaintiff’s laptop (as opposed to the information stored on that laptop). It is otherwise dismissed.

¹² Defendants claim a ruling in Plaintiff’s favor would “criminaliz[e] deletion of emails,” which would be an “absurd result.” (Dkt. 38 at 15.) But the statute explicitly prohibits “[d]eleting . . . any computer program or data,” including emails. O.C.G.A. § 16-9-93(b)(1). And it is not hard to imagine circumstances in which email deletion could be both sinister and harmful.

VII. Count 6

Count 6 claims Defendants Barkoff and Droege breached their fiduciary duties to Plaintiff. (Dkt. 1 ¶ 125.) Defendants say this count should be dismissed because it is preempted by GTSA and fails to state a claim. (Dkt. 31 at 33–35.) The Court partly agrees on the first issue (preemption) but disagrees on the second (failure to state a claim).

A. Preemption

Plaintiff's GTSA and breach-of-fiduciary claims both allege Defendants wrongfully downloaded Plaintiff's trade secret-information, misappropriated trade secrets by stealing a company laptop, and used trade secrets to compete against Plaintiff. (Dkt. 1 ¶¶ 70–71, 82, 125.) So GTSA preempts these portions of Count 6. *See Argos*, 2019 WL 4125968, at *12 (finding GTSA preemption because “Plaintiff relies on the same factual allegations of misappropriation for its . . . breach of fiduciary duty claims as its GTSA claim. Specifically, Plaintiff relies on facts that Young used Plaintiff's computer system to misappropriate Plaintiff's proprietary information.”).

But Count 6 also alleges Defendants “[w]rongfully plott[ed] to steal and misuse” Plaintiff's information, “cover[ed] up their theft by deleting

emails,” and “[w]rongfully delet[ed] files and data.” (Dkt. 1 ¶ 125.) Plaintiff’s GTSA claim does not rely on these allegations. So Count 6 survives GTSA preemption to that extent. As with Count 5, it also survives to the extent it seeks relief for laptop theft as opposed to theft of the information stored on that device.¹³

B. Merits

Of Plaintiff’s four non-preempted theories, Defendants move to dismiss only one as implausibly pled: the “plotting” theory. (Dkt. 31 at 34–35.)¹⁴ That theory claims Defendants breached their fiduciary duties

¹³ Count 6 asserts in conclusory fashion that Defendants “solicited RoadSync employees to leave with them and to compete against RoadSync before they were terminated.” (Dkt. 1 ¶ 126.) But, as Defendants point out, the complaint’s more specific allegations say the solicitation occurred *after* Defendants’ termination. (Dkt. 31 at 35.) The specific trumps the general, so the Court assumes any solicitation post-dated Defendants’ termination. That is fatal because “a breach of duty claim predicated on acts after [an employee’s] resignation must necessarily fail.” *NuVasive, Inc. v. Miles*, 2020 WL 5106554, at *14 (Del. Ch. Aug. 31, 2020); see *Touch of Italy Salumeria & Pasticceria, LLC v. Bascio*, 2014 WL 108895, at *7 (Del. Ch. Jan. 13, 2014) (“[G]enerally, no [fiduciary] duties exist once the fiduciary relationship has ended.”).

¹⁴ Defendants’ reply brief includes a one-sentence attack on Plaintiff’s deletion theories. (Dkt. 38 at 16.) But “[a]rguments raised for the first time in a reply brief are not properly before a reviewing court.” *United States v. Coy*, 19 F.3d 629, 632 n.7 (11th Cir. 1994). Defendants never mention the laptop theft specifically, though some of their briefing could be read to challenge it. Either way, the Court believes the laptop theory

by secretly *planning* the coordinated theft, deletion, and misuse of Plaintiff's trade secrets. (See Dkt. 1 ¶¶ 3, 46.) Defendants say this theory should be dismissed because, under Delaware law (which governs), "plotting cannot constitute a breach of fiduciary duty as a matter of law." (Dkt. 31 at 35.) But that is wrong. The law is not so absolute. See *Sci. Accessories Corp. v. Summagraphics Corp.*, 425 A.2d 957, 965 (Del. 1980) ("The right to make arrangements to compete is *by no means absolute* and the exercise of the privilege may . . . rise to the level of a breach of an employee's fiduciary duty." (emphasis added)).

Instead, as Defendants' own citation shows, "[a]n agent can make arrangements or preparations to compete with his principal before terminating his agency, *provided he does not act unfairly or injure his principal.*" (Dkt. 31 at 35 (emphasis added).) This means an "employee [cannot] commit[] some fraudulent, unfair or wrongful act in the course of preparing to compete in the future." *Sci. Accessories*, 425 A.2d at 965; see *Seibold v. Camulos Partners LP*, 2012 WL 4076182, at *21 (Del. Ch.

plausibly alleges a fiduciary breach. See *Beard Rsch., Inc. v. Kates*, 8 A.3d 573, 603 (Del. Ch. 2003) (finding fiduciary breach where plaintiff retained company property—including "computer disks"—after his resignation).

Sept. 17, 2012) (“An agent may . . . take steps to prepare to compete with his principal, so long as these steps are ‘not otherwise wrongful.’” (quoting Restatement (Third) of Agency § 8.04)). If an employee does engage in “concerted action designed with the purpose of leaving [his employer] in the lurch,” he may have breached his fiduciary duties. Restatement (Third) Of Agency § 8.04 cmt. b.

Given these principles, Defendants’ blanket statement—that “plotting cannot constitute a breach of fiduciary duty as a matter of law”—is simply untrue. Plotting can constitute a breach. Of course, whether the plotting here actually *did* breach Defendants’ fiduciary duties is a different question. But Defendants do not address that issue. So the Court need not resolve it. Besides, “the ultimate determination of whether an employee has breached his fiduciary duties to his employer by preparing to engage in a competing enterprise must be grounded upon a thoroughgoing examination of the facts and circumstances of the particular case.” *Sci. Accessories*, 425 A.2d at 965. And that kind of fact-intensive inquiry may be better suited for summary judgment anyway.

Given the record here, including Defendants’ narrow argument for dismissal, Plaintiff’s plotting theory can proceed.

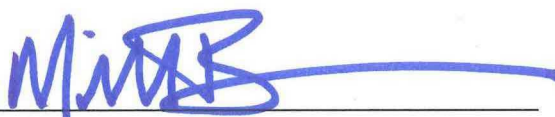
C. Conclusion

Count 6 can proceed to the extent it alleges Defendants “[w]rongfully plott[ed] to steal and misuse” Plaintiff’s information, “cover[ed] up their theft by deleting emails,” “[w]rongfully delet[ed] files and data,” and stole or converted Plaintiff’s laptop (as opposed to the information on that laptop). (Dkt. 1 ¶ 125.) It is otherwise dismissed.¹⁵

VIII. Conclusion

Defendants’ Motion to Dismiss (Dkt. 31) is **GRANTED IN PART** and **DENIED IN PART**. Counts 1, (DTSA), 2 (GTSA), 5 (GCSPA), and 6 (fiduciary duty) can proceed in part. Counts 3–4 (breach of contract) can proceed in full. Defendants Does 1–10 are **DISMISSED**.

SO ORDERED this 30th day of September, 2022.



MICHAEL L. BROWN
UNITED STATES DISTRICT JUDGE

¹⁵ The Court briefly flags a wrinkle that no one raised. Delaware law governs Plaintiff’s fiduciary duty claim. But GTSA only preempts “laws of *this state*.” O.C.G.A. § 10-1-767(a) (emphasis added). If GTSA preemption is limited to *Georgia* laws, and Plaintiff’s fiduciary claim arises under *Delaware* law, how can GTSA preempt the fiduciary claim? No one explores this. So neither does the Court.